A METHOD OF PROCESSING PAYMENT ON A
NETWORK OF COMPUTERS SUCH AS THE INTERNET

MoneyIN
Docket No. 1475B.5A.5

"SPEC475B.5A5"

March 22, 2002

Sub/spec

A METHOD OF PROCESSING PAYMENT ON A

NETWORK OF COMPUTERS SUCH AS THE INTERNET

1   Background of the Invention:

2       This is a continuation of United States Patent application

3   serial number 09/400,724, filed on September 21, 1999, and

4   entitled "Financial System of Computers";which was a continuation

5   of United States Patent application serial number 09/166,749

6   filed on October 5, 1998, and entitled "Financial System of

7   Computers", now United States Patent number 5,963,917; which was

8   a continuation of United States Patent application serial number

9   08/597,017, entitled "An Improved Financial Transactions System"

10  filed February 5, 1996, now United States Patent number

11  5,822,737, issued on October 13, 1998.

12      This invention relates generally to financial transactions

13  and more particularly to transactions involving credit or debit

14  cards.

15      The time is fast approaching where a significant amount of

16  commerce will be conducted using distributed networks of

17  computers such as the Internet.  The reason this ground-swell of

18  commerce will occur is the ability of a single merchant to

19  economically reach a vast number of potential customers at

1   substantially no costs.   Further, the customers are able to

2   review a great number of vendors and their products with the ease

3   of a few key strokes and clicks of the mouse.

4       Although there are vast numbers of merchants already using

5   such networks, the sales volume has been particularly low due to

6   a variety of reasons.   One reason which has depressed commerce on

7   the networks, is the difficulty with which customers can pay for

8   their purchases.

9       A variety of techniques have been developed to cure this

10  problem ranging from accepting phone orders to the establishment

11  of another currency called "E-Cash".

12      Phone orders in response to merchant promotional materials

13  creates a variety of problems.   One major problem is the

14  requirements for phone lines and personnel to receive and process

15  the phone orders.   Another hurdle is the simple fact that most

16  customers have a single phone line to their residence and this

17  line is used by the computer for accessing the network; the

18  customer has to disconnect from the network to make the phone

19  order.

20      Although E-Cash is a viable alternative, it is faced with

21  some enormous problems which will be difficult or impossible to

22  address.   These include:   counterfeiting problems; government

23  reluctance to accept the concept; difficulties in getting access

24  for handling E-Cash; and, the low number of users and merchants

1    which can use E-Cash.

2          It is clear from the foregoing that there is a need for an

3    efficient methodology and system to accept payment over

4    distributed computer networks.

## Summary of the Invention:

The present invention contemplates a totally automated system for securing payment via a distributed network of computers. In this context, the invention creates an automated payment system particularly suited for purchases over a network such as the Internet.

Although the present invention is described relative to the Internet, its application is not so limited and is intended to be used on any distributed computer system in which merchants and consumers interact for the purpose of supplying and purchasing goods or services.

In such a distributed computer network, a merchant or vending computer contains certain promotional information which is communicated to a customer's computer. This information is intended to give the customer sufficient information to make a decision on if the goods/services are acceptable.

As used within this discussion, the term "merchant computer" signifies a computer system which is used for the purpose of selling goods or services. The vendor itself does not necessarily own the computer; in some situations, the computer is operated on behalf of the merchant or vendor.

Based upon the promotional information, the consumer/operator of the customer's computer decides to purchase the services or goods described by the promotional information.

1     It is at this point where the present invention is

2    particularly powerful as it provides a simple, easy, methodology

3    and linkage for the customer to pay for the goods/services.

4     In this context, the customer's computer is linked to a

5    payment processing computer and the customer's credit card number

6    and the amount of the goods or services is transmitted to the

7    payment processing computer.  For security reasons, an encrypting

8    software package is first downloaded to the customer's computer

9    so that the credit card number is secure from "hackers" who might

10   also be on the network.

11    Although the term "credit card" is used, the invention

12   covers the use of any type of financial guarantee card such as

13   automatic debit accounts, checking account numbers, savings

14   account numbers, and other such devices obvious to those of

15   ordinary skill in the art.

16    The payment processing computer automatically contacts a

17   bank for verification of the credit card and amount; the bank

18   transmits an authorization to the payment processing computer.

19   This authorization, usually in the form of a number, is stored

20   within the payment processing computer's memory for later

21   reference.

22    The link or connection with the bank is terminated by the

23   payment processing computer and the payment processing computer

24   turns its attention to the customer's computer.  The payment

1  processing computer communicates a self-generated transaction

2  indicia, and in some embodiments a password, to the customer's

3  computer.

4      The transaction indicia is generated by the payment

5  processing computer for proper record keeping.  The transaction

6  indicia is also used by the customer to verify that an order has

7  been generated and accepted.

8      The password is defined by the merchant's computer for the

9  payment processing computer to pass along to the customer's

10  computer.  The password is used by the customer's computer to

11  gain access to restricted material within the merchant's

12  computer.

13      As example, assume the merchant's computer is supplying

14  information as to genealogy.  As an initial process, the customer

15  enters the name being researched and receives a preliminary

16  report on the genealogy (the promotional material).  To proceed

17  though, and get the actual data, the customer must pay to access

18  this further information.

19      To do so, the customer links with the payment processing

20  computer, and in the manner outlined above, receives back the

21  transaction indicia and the password.  The payment processing

22  computer links the customer computer back to the merchant

23  computer; the customer provides the password to the merchant's

24  computer and is given access to the full genealogy report.

1    As outlined in this example, in the embodiment where a

2    password is used, the customer's computer uses the password with

3    the merchant's computer in obtaining access to protected

4    information or to establish shipping instructions.

5    The re-linking of the customer computer to the merchant

6    computer is accomplished in a variety of ways.  In the preferred

7    embodiment, the payment processing computer obtains the

8    merchant's address or Unique Recognition Location (URL) from the

9    customer computer when the customer connects with the payment

10   processing computer.  This URL is used in a variety of ways, to

11   identify the merchant, to establish the amount of the

12   product/service, and to establish the return URL when the payment

13   processing computer is done with its task for the customer

14   computer.

15   By selective use of the URL on the merchant's part, the URL

16   transmits a tremendous amount of information to the payment

17   processing computer.  As example, assume the URL for the home-

18   page of the merchant is: merchant.com/widget.

19   When the merchant is selling a single product (a widget),

20   this URL is easy to match to the product.  When the merchant

21   wants to sell a variety of widgets, then for a blue widget, the

22   URL might be: merchant.com/widget/blue.

23   In some embodiments, the customer's computer is not linked

24   back to the originating URL of the Merchant computer but rather

1    to another URL.  The return URL is stored in the payment

2    processing computer and is used when the Merchant wants the

3    customer/consumer to be passed back to a different location (i.e.

4    where the restricted access information is accessible, or to

5    inform the consumer that their card has been rejected).

6         The invention, together with various embodiments thereof,

7    will be more fully explained by the accompanying drawings and the

8    following descriptions.

1 <u>Drawings in Brief:</u>

2       Figures 1A and 1B are block diagrams of the two computer

3 configurations used in the preferred embodiment.

4       Figure 1C is a graphical representation of the preferred

5 memory organization for the computer illustrated in figure 1A.

6       Figures 2A, 2B, 2C, 2D, and 2E graphically illustrate the

7 connections and disconnections of the preferred order.

8       Figures 3A, 3B, 3C, and 3D are frontal views of one

9 embodiment of a consumer's display screen.

10       Figure 4A is a flow-chart of the preferred embodiment's

11 payment processing operation.

12       Figure 4B is a flow-chart of an alternative embodiment's

13 payment processing operation.

14       Figure 5 is a flow-chart of the operation of the merchant's

15 computer.

16

17

1 <u>Drawings in Detail:</u>

2      Figures 1A and 1B are block diagrams of the two computer

3 configurations used in the preferred embodiment.

4      Figure 1A illustrates the configuration of the preferred

5 payment processing computer.  As shown, computer 10A is a simple

6 layout of a Central-Processing-Unit (CPU) 11A which uses both

7 non-volatile memory 12A and Random-Access-Memory (RAM) 13A.

8      Communication to and from CPU 11A is via modem 14A which

9 communicates with other computers via the network connected by

10 phone line 15A.

11      Computer 10B, illustrated in figure 1B, shows the preferred

12 computer configuration used for the merchant computer and the

13 customer computer.  Again, CPU 11B is connected to memories RAM

14 13B and non-volatile memory 12B.  In the case of the merchant

15 computer, the promotional material is stored on non-volatile

16 memory 12B and is retrieved and communicated by CPU 11B using

17 modem 14B and phone line 15B.

18      This system is able to communicate with an operator via

19 monitor 16 for visual information.  Monitor 16 is used for the

20 perusal of the promotional material by the customer.

21      Keyboard 17 is used to communicate operator commands to CPU

22 11B.  In like fashion, mouse input device 18 is also used for

23 operator input to CPU 11B.

24      Optional printer 19 is used to create a hard copy of the

1    material being displayed to the operator/customer via monitor 16.

2        The differences between the computers shown in figure 1A and

3    1B are pronounce since the payment processing computer of figure

4    1A does not require input or direction from a human operator.

5    Rather, in the preferred embodiment, the payment processing

6    computer runs totally automatically and collects all of the data

7    and information it requires for its operation automatically from

8    the computers with which it is linked and with what is stored in

9    its memory.

10       Figure 1C is a graphical representation of the preferred

11   memory organization for the computer illustrated in figure 1A.

12       Memory 9, located preferably in non-volatile memory 12A, has

13   three sections.  The first section 8A is the product listing

14   reference which is composed of multiple groupings.   This data

15   remains relative constant and is defined by the merchant.  Each

16   grouping, such as 7A, includes data identifying:

17           Part Number

18           Merchant Identification

19           Cost of Product/Service

20           Description of the Product/Service

21           Authorized Return URL

22           Rejected Return URL

23           Password

24       The second section is for defining the merchant's

1    information.    Each grouping 7B within section 8B contains

2    relative constant information such as:

3                Merchant Identification

4                Business Name

5                Contact Name within the Business

6                Business Address

7                E-Mail address for the Business

8                Bank Checking Number for the Business

9        The third section 8C is an accounting listing which is

10    constantly up-graded as new payments are processed.    This section

11    is used for making full accounting to the various merchants.

12    Grouping 7C within section 8C contain:

13                Transaction Number

14                Date of transaction

15                Amount of the transaction

16                Part number involved in transaction

17                Credit Card Number

18                Authorization Number

19        The authorization number is the indicia received from the

20    bank indicating that the credit card charge has been accepted.

21        The use of memory 9 allows the payment processing computer

22    to have access to the necessary information to handle the linkage

23    and perform the proper accounting.

24        Figures 2A, 2B, 2C, 2D, and 2E graphically illustrate the

1    connections and disconnections of the preferred order.

2    Referring to figure 2A, in a typical fashion, a consumer via

3    customer computer 21 enters the network 20 and searches through

4    various merchant computers until the consumer locates the

5    merchant of choice and connects with merchant computer 22.

6    Merchant computer 22 communicates the promotional material via

7    network 20 to customer computer 21.

8    When the consumer decides to buy the service or product from

9    merchant 22, as shown in figure 2B, the link with merchant

10   computer 22 is broken and customer computer 21 links with the

11   payment processing computer 23.  In the change from merchant

12   computer 22 to payment processing computer 23, an indicia of the

13   URL or the product being promoted by merchant computer 22 is

14   communicated to the payment processing computer 23.

15   The indicia as a URL of the last site is available through

16   normal network operations and its handling is obvious to those of

17   ordinary skill in the art.  The product number is easily

18   combined with the URL; thereby making the product number also

19   available to the payment processing computer 23.

20   In some embodiments, the originating URL is crossed checked

21   to a memory data base to achieve the product number.  In this

22   embodiment, the merchant structures its material so that only a

23   single product/service is associated with a specific URL.

24   Using the product number (or developing the product number

1  from the merchant's URL), the payment processing computer is able

2  to cross reference its own memory (as described earlier) to

3  achieve other important information including:  the amount of the

4  product/service, a description of the product/service, the name

5  and address of the merchant, and other which will be used in

6  later operations.

7       The payment processing computer 23 accepts from the customer

8  computer 21, the credit card account number which is to be

9  debited the amount of the product.

10      As shown in figure 2C, in this embodiment, while maintaining

11 linkage with the customer computer 21, the payment processing

12 computer 23 establishes a link via phone lines 25 with the credit

13 card server computer 24.  The credit card account number and

14 amount is communicated to the credit card server computer 24

15 which responds to the payment processing computer 23 with an

16 authorization indicia.  This authorization indicia gives the

17 acceptance or denial of the charge.

18      If a product is to be shipped, and if the charge has been

19 authorized, as shown in figure 2D, the payment processing

20 computer 23 connects with the merchant computer 22 and directs

21 the merchant to ship the product to the consumer.

22      As shown in figure 2E, since the payment processing computer

23 23 has identified the product number, it is able to retrieve from

24 its memory the URL for reconnecting the customer computer 21 with

14

1  the merchant computer 22. In this manner, the entire operation

2  is totally transparent to the consumer since they feel they have

3  been continuously working with the merchant computer 22.

4      Further, using the URL's from its memory, the payment

5  processing computer 23 is able to link the customer computer 21

6  to the merchant computer 22 at an address which is different from

7  where the consumer was originally connected. In this manner, the

8  payment processing computer 23 is able to direct the consumer to

9  different locations which are consistent with the authorization

10  indicia (accept/reject) on their credit card.

11      As example, assume, the credit card was authorized, then the

12  consumer could be reconnected to an area which has restricted

13  access so that the consumer can gain the information paid for; if

14  on the other hand, the credit card was rejected, the connection

15  would be to a page indicating such and possibly asking for

16  another card number.

17      In this manner, the payment processing computer 23 is able

18  to control the operation and interface between the customer

19  computer 21 and the merchant computer 22.

20      Periodically, the payment processing computer 23 connects

21  via the phone lines 25 with the credit card server 24 and

22  instructs it to transfer the appropriate amount of funds to the

23  merchant's bank computer 26 so that the merchant has access to

24  the funds paid for his product/service provided to the consumer.

1    Figures 3A, 3B, 3C, and 3D are frontal views of one

2    embodiment of a consumer's display screen.

3    Screen 30A is designed to provide the promotional

4    information so that the consumer is attracted to purchase the

5    product.  In screen 30A is the name of the merchant company (XYZ

6    CO.) 31, the name of the product (widget) 32, the price ($14.95)

7    33, and the part number (#10234) 34.

8    Also located on screen 30A is a software key 35 which allows

9    the consumer to pay for the product.  In this embodiment, by

10   activating this software key 35 (typically through a click of the

11   mouse), screen 30A is changed to screen 30B which is identical

12   except that the software key 35 has been replaced with an order

13   window 36.

14   Order window 36 allows the consumer to complete the

15   necessary information to order the product.  This includes the

16   part number 37A, the amount 37B, and the credit card number 37C.

17   When the consumer is ready, the software key "Send" 37D or the

18   software key "Cancel" 37E is activated.  In the case of a cancel,

19   the screen returns to screen 30A.

20   In a "send"  37D, mode, the payment processing computer

21   contacts the bank computer and determines if the credit card is

22   valid and if the amount is available.  If the charge is

23   authorized, the screen changes to 30C in which the order window

24   36 has been replaced with authorization window 38 which shows

1   that the charge has been accepted 39A, the transaction no.

2   (A1483) 39B, and the password ("GO") 39C which the consumer is to

3   use with the merchant.

4      When this information has either been printed or committed

5   to memory, the consumer activates software key 39D to "Proceed"

6   to screen 30D.  At this point, the consumer is able to enter the

7   password 29 so that the restricted access is lifted.  In the

8   genealogy example, it is at this point the consumer gains access

9   to the full report.

10     Figure 4A is a flow-chart of the preferred embodiment's

11  payment processing operation.

12     After start 40A, a connection is made with the customer

13  computer 41A and the encryption software is downloaded to the

14  customer computer 41B.  Encryption software is preferably used

15  for transmittal of the credit card number so that the integrity

16  of the card is not jeopardized.

17     The consumer computer then communicates, and the payment

18  processing computer accepts, the account number, the amount, and

19  the identification of the product or service, 42A.  A connection

20  is made with the credit card server 41C and the account number

21  and amount is transmitted 41D to the credit card server over the

22  established phone lines.  In response to this query, the

23  authorization data is received 42B and the connection with the

24  credit card server 41E is broken.

1     A transaction indicia is generated 41F. This transaction

2    indicia is not the authorization data but serves as an internal

3    monitoring system for the payment processing computer so that the

4    accounting is kept accurate.

5     From the memory, the password is withdrawn 41G for the

6    product so ordered; and, the password and transaction indicia is

7    transmitted to the customer computer 41H.

8     At this point, the connection with the customer computer is

9    terminated 41I and the program stops 40B.

10    Figure 4B is a flow-chart of an alternative embodiment's

11   payment processing operation.

12    After start 43A, the program connects with the customer

13   computer 44A and at the same time obtains the merchant URL 45A.

14   Using the merchant URL, the payment processing computer searches

15   its memory and identifies the merchant number, the part number,

16   and the purchase amount 44B.

17    The encryption software is downloaded into the customer

18   computer 44C and the credit card account number is received 45.

19   A connection is then made with the credit card server computer

20   44D and the account number and the amount is transmitted 44E.

21   This inquiry results in an authorization code 45C being received

22   and the connection with the credit card server being broken 44F.

23    A check is then made to see if the credit card purchase was

24   authorized 46A.

1    If the credit card purchase was denied, the URL to use for a

2    rejection is withdrawn from memory 44G and the Customer computer

3    is connected to the merchant computer at this URL 44H leaving the

4    payment processing computer able to disconnect 44I and stop 43B.

5    Should the credit card purchase be accepted, 46A, then the

6    program generates a transaction identification 44J.  This

7    transaction identification is stored along with the date, amount

8    of purchase, and the merchant number 44K.

9    The password is retrieved from memory 44L and it, together

10   with the transaction identification, is transmitted to the

11   customer computer 44M.

12   From memory, the authorized URL is withdrawn 44N.

13   A determination, based upon stored data, is made as to the

14   character of the product (service or goods) 46B.  If the product

15   relates to goods which are to be shipped, a shipping order

16   including the transaction identification, the amount, the date,

17   and address of the customer, is communicated to the merchant 44O

18   to satisfy the order.  If the product is a "service", the program

19   skips to step 44P.

20   The customer computer is then connected to the authorized

21   URL 44P and the connection with the customer computer is

22   terminated 44Q allowing the program to stop 43C.

23   Figure 5 is a flow-chart of the operation of the merchant's

24   computer.

1      After start 50A, the merchant computer connects with the

2    customer computer 51A and communicates the promotional material

3    52A.  The password is received from the customer 52B and is

4    checked to see if it is the correct password 53A.

5      If the password is incorrect, a determination is made on if

6    it is the customer's first try 53B; if it is, then the customer

7    is given another chance to enter the correct password 52B.  If

8    the customer has tried twice to enter the correct password, the

9    connection with the customer is terminated 51C and the program

10   stops 50C.

11      If the password is correct, 53A, then the secure or

12   restricted access data is communicated to the customer's computer

13   51D and the connection with the customer's computer is terminated

14   51B.  The program then stops 50B.

15      In this manner, secure information is selectively

16   transmitted to a customer's computer upon the presentation of a

17   password.

18      It is clear from the foregoing that the present invention

19   creates a highly improved system for acceptance and processing of

20   payments over a distributed computer network.

21